# The Group of Units of the Integral Group Ring $\mathbb{Z}D_4$*

CÉSAR POLCINO MILIES

**Introduction and Notation.** The study of the multiplicative group of a group ring started in 1940 with a well-known paper due to G. Higman [3]. Many results on this topic have been published in recent years; however, few examples have been computed.

Recently, Hughes and Pearson [4] studied the group of units of the integral group ring $\mathbb{Z}S_3$, where $S_3$ is the symmetric group on three symbols. Using similar methods we study here the group of units of the integral group ring $\mathbb{Z}D_4$ where $D_4$ stands for the Dihedral Group of eight elements; i.e. the group with two generators a and $b$ and relations:

$$a^4 = b^2 = baba = 1$$

For an arbitrary group $G$ we introduce the following notation: $U(\mathbb{Z}G)$ will stand for the group of units of the group ring $ZG$. The elements of the form $\pm g$, with $g$ in $G$, are the *trivial units* of $\mathbb{Z}G$.

The homomorphism $\varepsilon: \mathbb{Z}G \longrightarrow \mathbb{Z}$ such that $\varepsilon(g) = 1$ for every $g$ in $G$ is called the *augmentation function.* We denote by $V(\mathbb{Z}G)$ the normal subgroup of units $u \in \mathbb{Z}G$ such that $\varepsilon(u) = 1$. An element $u$ in $V(\mathbb{Z}G)$ is called a *normalized unit*. Finally, an automorphism $\theta$ of $\mathbb{Z}G$ is said to be *normalized* if $\varepsilon \circ \theta(g) = 1$ for all $g$ in $G$.

The following questions were raised in [4]:

(a) Is every unit of finite order in $\mathbb{Z}G$ conjugate to a trivial unit?

(b) What are the maximal finite subgroups of $U(\mathbb{Z}G)$?

(c) Is every normalized automorphism of $\mathbb{Z}G$ the product of an inner automorphism and an automorphism of $G$?

*Recebido pela SBM em 12 de setembro de 1974.

We answer these questions in connection to this particular case. A brief communication of these results was published in [6].

**1. The Group of Units.** It is well-known that there exists an isomorphism:

(1) $$\phi\colon \mathbb{Q}D_4 \longrightarrow \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus M_2(\mathbb{Q})$$

where $M_2(\mathbb{Q})$ stands for the full ring of $2 \times 2$ matrices over the field of rational numbers, such that:

(2) $$\phi(a) = \left(1,\ 1,\ -1,\ -1,\ \begin{vmatrix} 0 & -1 \\ 1 & 0 \end{vmatrix}\right)$$
$$\phi(b) = \left(1,\ -1,\ 1,\ -1,\ \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix}\right)$$

Consider $D_4$ as a $\mathbb{Q}$-basis of $\mathbb{Q}D_4$ and the canonical basis of the direct sum. Regarding $\phi$ as a $\mathbb{Q}$-isomorphism, we readily see that its matrix with respect to these bases is:

$$A = \begin{vmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 0 & -1 & 0 & 0 & -1 & 0 & 1 \\ 0 & -1 & 0 & 1 & 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 & 1 & 0 & -1 & 0 \\ 1 & 0 & -1 & 0 & 0 & 1 & 0 & -1 \end{vmatrix} \quad \text{with } A^{-1} = \frac{1}{8} \begin{vmatrix} 1 & 1 & 1 & 1 & 2 & 0 & 0 & 2 \\ 1 & 1 & -1 & -1 & 0 & -2 & 2 & 0 \\ 1 & 1 & 1 & 1 & -2 & 0 & 0 & -2 \\ 1 & 1 & -1 & -1 & 0 & 2 & -2 & 0 \\ 1 & -1 & 1 & -1 & 0 & 2 & 2 & 0 \\ 1 & -1 & -1 & 1 & -2 & 0 & 0 & 2 \\ 1 & -1 & 1 & -1 & 0 & -2 & -2 & 0 \\ 1 & -1 & -1 & 1 & 2 & 0 & 0 & -2 \end{vmatrix}$$

From the expression of $A^{-1}$ it follows that an element

$$\chi = \left(x_1,\ x_2,\ x_3,\ x_4,\ \begin{vmatrix} x_5 & x_6 \\ x_7 & x_8 \end{vmatrix}\right) \in \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus M_2(\mathbb{Z})$$

belongs to $\phi(\mathbb{Z}D_4)$ if and only if:

(3) $$x_1 + x_2 + x_3 + x_4 + 2x_5 + 2x_8 \equiv 0 \pmod 8$$

and seven other congruence equations obtained from the rows of $A^{-1}$ are satisfied.

Reducing this system we see that it is equivalent to the following:



(4)
$$\begin{array}{ll} \text{(i)} & x_1 + x_2 + x_3 + x_4 + 2x_5 + 2x_8 \equiv 0 \pmod 8 \\ \text{(ii)} & x_2 + x_3 + 2x_8 \equiv 0 \pmod 4 \\ \text{(iii)} & x_3 - x_4 - x_5 - x_6 - x_7 + x_8 \equiv 0 \pmod 4 \\ \text{(iv)} & x_4 + x_5 + x_7 \equiv 0 \pmod 2 \\ \text{(v)} & x_5 + x_8 \equiv 0 \pmod 2 \\ \text{(vi)} & x_6 + x_7 \equiv 0 \pmod 2 \end{array}$$

If we also want $\chi$ to belong to $\phi(U(\mathbb{Z}D_4))$ we see that we must have $x_i = \pm 1$, $i = 1, 2, 3, 4$ and $x_5x_8 - x_6x_7 = \pm 1$.

An elementary computation shows that given a matrix $X = \begin{vmatrix} x_5 & x_6 \\ x_7 & x_8 \end{vmatrix}$ in $\mathbf{GL}(2, \mathbb{Z})$ verifying equations (v) and (vi) of (4) there exist $x_i$, $i = 1, 2, 3, 4$ such that $X = (x_1, x_2, x_3, x_4, X) \in \phi(U(\mathbb{Z}D_4))$ if and only if one of the following conditions also holds:

(5) (i) $x_8 \equiv 1 \pmod 2$; $x_5 + x_6 + x_7 - x_8 \equiv 0 \pmod 4$; $x_5 + x_8 \equiv 2 \pmod 4$
(ii) $x_8 \equiv 1 \pmod 2$; $x_5 + x_6 + x_7 - x_8 \equiv 2 \pmod 4$; $x_5 + x_8 \equiv 0 \pmod 4$
(iii) $x_8 \equiv 0 \pmod 2$; $x_5 + x_8 \equiv 0 \pmod 4$

We shall note by $\Omega$ the subgroup of $\mathbf{GL}(2, \mathbb{Z})$ formed by those matrices verifying conditions (v) and (vi) of (4) and any one of the conditions in (5). For any element $X \in \Omega$ the same computation shows that there exist exactly two elements in $\phi(U(\mathbb{Z}D_4))$ whose last component is $X$. In fact, if $\delta = \pm 1$ and $X$ is in $\Omega$ we have:

(6) If (i) of (5) holds, then $\chi = (\delta, \delta, \delta, \delta, X) \in \phi(U(\mathbb{Z}D_4))$.
If (ii) of (5) holds, then $\chi = (\delta, \delta, -\delta, -\delta, X) \in \phi(U(\mathbb{Z}D_4))$.

Finally, if (iii) of (5) holds, we must consider two cases:

(a) If $x_5 + x_6 + x_7 - x_8 \equiv 0 \pmod 4$ also holds, then

$$\chi = (\delta, \delta, -\delta, -\delta, X) \in \phi(U(\mathbb{Z}D_4)).$$

(b) If $x_5 + x_6 + x_7 - x_8 \equiv 2 \pmod 4$ holds, then

$$\chi = (\delta, -\delta, \delta, -\delta, X) \in \phi(U(\mathbb{Z}D_4)).$$

If $\alpha \in U(\mathbb{Z}D_4)$ is such that $\phi(\alpha) = (x_1, x_2, x_3, x_4, X)$, it is easy to see that:

$$\varepsilon(\alpha) = x_1 . \tag{7}$$

Hence, for any $X \in \Omega$ there exists only one element in $\phi(V(\mathbb{Z}D_4))$ whose last component is $X$. Thus:

$$V(\mathbb{Z}D_4) \simeq \Omega \quad \text{and} \quad U(\mathbb{Z}D_4) \simeq \{\pm 1\} \times \Omega. \tag{8}$$

Now we collect some information about $\Omega$. First it can be shown that

$$[GL(2, \mathbb{Z}) : \Omega] = 6.$$

Actually:

$$w_1 = \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix}, \quad w_2 = \begin{vmatrix} 1 & 2 \\ 0 & 1 \end{vmatrix}, \quad w_3 = \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix},$$

$$w_4 = \begin{vmatrix} 1 & 1 \\ 2 & 1 \end{vmatrix}, \quad w_5 = \begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix}, \quad w_6 = \begin{vmatrix} 1 & 2 \\ 1 & 1 \end{vmatrix},$$

is a complete set of representatives of the left cosets of $\Omega$ in $GL(2, \mathbb{Z})$.

We shall show that the elements of finite order in $\Omega$ can only have orders equal to 2 or 4. It is easy to see that an element of finite order in $\mathbf{GL}(2, \mathbb{Z})$ can only have order equal to 2, 3, 4 or 6. The result will then follow from:

PROPOSITION 1. *Let $G$ be a finite $p$-group. Then a normalized unit of finite order in $U(\mathbb{Z}G)$ has order a power of $p$.*

PROOF. Let $\alpha$ be a normalized unit of finite order in $\mathbb{Z}G$ and let $J_p$ be the field with exactly $p$ elements.

The natural homomorphism $\psi: \mathbb{Z} \longrightarrow J_p$ can be extended in the usual way to a homomorphism $\psi^*: U(\mathbb{Z}G) \longrightarrow U(J_pG)$ which carries $\langle\alpha\rangle$, the finite subgroup generated by $\alpha$, onto a subgroup of units of $J_pG$.

Now, if an element $x = \sum_i x_i g_i \in U(\mathbb{Z}G)$ belongs to $Ker(\psi^*)$ and $g_1$ stands for the identity element in $G$, then $x_1 = 1$.

Since every element in $\langle\alpha\rangle$ is of finite order, and Berman [1] has shown that an element of finite order in an integral group ring other than $\pm 1$ must be such that $x_1 = 0$, it follows that $\langle\alpha\rangle$ is isomorphic to its image in $V(J_pG)$.



Finally, if $G$ is a $p$-group, then:

$$V(J_pG) = \{v \in J_pG \mid \varepsilon(v) = 1\}$$

and a direct computation shows that:

$$|V(J_pG)| = p^{|G|-1},$$

thus every element has order a power of $p$.

**2. The Conjugacy Problem.** To give a negative answer to question (a) we shall study the conjugacy classes of elements of order 2 in $U(\mathbb{Z}D_4)$.

It is known that there are three such classes in $GL(2, \mathbb{Z})$. One of them is the class with one element $C_0 = \{-I\}$. The other two are:

$$C_1 = \left\{X = \begin{vmatrix} a & b \\ c & -a \end{vmatrix} \,\middle|\, a^2 + bc = 1;\ a \text{ odd};\ b, c \text{ even}\right\}$$

$$C_2 = \left\{X = \begin{vmatrix} a & b \\ c & -a \end{vmatrix} \,\middle|\, a^2 + bc = 1;\ X \notin C_1\right\}$$

(See [4]).

PROPOSITION 2. *There are five conjugacy classes of elements of order 2 in $\Omega$.*

PROOF. First, we shall see that an element $Y \in \Omega \cap C_1$ is conjugate either to $X_1 = \begin{vmatrix} 1 & 0 \\ 0 & -1 \end{vmatrix}$ or to $Y_1 = \begin{vmatrix} 1 & 4 \\ 0 & -1 \end{vmatrix}$ in $\Omega$.

In fact, there exists $u \in \mathbf{GL}(2, \mathbb{Z})$ such that $uYu^{-1} = X_1$. Since $u = w_i\alpha$ for some $\alpha$ in $\Omega$ and some $i = 1, \ldots, 6$, we have:

$$\alpha Y \alpha^{-1} = w_i^{-1} X_1 w_i . \tag{9}$$

If $i = 1$ then $u \in \Omega$ and we are done. If $i = 3, \ldots, 6$ we see that $w_i^{-1} X_1 w_i$ is not in $\Omega$ and equation (9) is impossible. Finally, $w_2^{-1} X_1 w_2 = Y_1$ and it is easy to see that $X_1$ and $Y_1$ are not conjugate in $\Omega$.

It can be shown in the same way that an element $Y \in \Omega \cap C_2$ is conjugate either to $X_2 = \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix}$ or to $Y_2 = \begin{vmatrix} -2 & -3 \\ 1 & 3 \end{vmatrix}$ in $\Omega$. These two elements are not conjugate in this group.

COROLLARY. *Not every normalized unit of finite order is conjugate to an element in* $D_4$.

PROOF. Let $\pi$ be the natural projection of the direct sum onto $M_2(\mathbb{Q})$. The elements of order two in $D_4$ are: $a^2$, $b$, $a^2b$, $a^3b$. But: $\pi \circ \phi(a^2) = -I$; $\pi \circ \phi(b)$, $\pi \circ \phi(a^2b) \in X_1\Omega$; $\pi \circ \phi(ab)$, $\pi \circ \phi(a^3b) \in X_2\Omega$.

Thus the elements $\alpha$ in $V(\mathbb{Z}D_4)$ such that $\pi \circ \phi(\alpha)$ belongs either to $Y_1\Omega$ or to $Y_2\Omega$ are normalized units of order two and they are not conjugate to an element in $D_4$.

**3. The Maximal Subgroups.** After the preceeding results, in order to answer question (b) we need only to study the maximal finite subgroups of $\Omega$.

It follows from well-known results about the finite subgroups of $\mathbf{GL}(2, \mathbb{Z})$ (see [5] Chapter IX § 14) and Proposition 1, that any maximal subgroup of $\Omega$ is conjugate in $\mathbf{GL}(2, \mathbb{Z})$ to the subgroup $D_4^*$ of $\Omega$ generated by

$$A = \begin{vmatrix} 0 & -1 \\ 1 & 0 \end{vmatrix} \quad \text{and} \quad B = \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix}.$$

Let $\Gamma$ be such a subgroup and let $V \in GL(2, \mathbb{Z})$ be a matrix such that

$$\Gamma^V = V\Gamma V^{-1} = D_4^*. \tag{10}$$

Then, we can choose generators $X$, $Y$ of $\Gamma$ such that

$$X^V = A, \qquad Y^V = B. \tag{11}$$

Since $Y \in C_2$, it is conjugate in $\Omega$ either to $X_2 = B$ or to $Y_2$.

Suppose first that there exists $U$ in $\Omega$ such that

$$Y^U = B \tag{12}$$

From (11) and (12) it follows easily that

$$U^{-1}V \in Z(B) = \{\pm I, \pm B\}$$

the centralizer of $B$ in $\mathbf{GL}(2, \mathbb{Z})$, thus

$$V = \pm U \quad \text{or} \quad V = \pm UB. \tag{13}$$

In both cases $\Gamma$ and $D_4^*$ are conjugate in $\Omega$.



Now, if there exists $U$ in $\Omega$ such that

$$Y^U = Y_2 \tag{14}$$

it can be seen in a similar way that

$$VU^{-1}W^{-1} \in Z(B),$$

where $W = \begin{vmatrix} 1 & 2 \\ 0 & 1 \end{vmatrix} \in \mathbf{GL}(2, \mathbb{Z})$ is such that $Y_2^W = B$. Thus we obtain:

$$V = \pm WU \quad \text{or} \quad V = \pm BWU. \tag{15}$$

In the first case we have:

$$X^U = W^{-1}AW = \begin{vmatrix} -2 & -5 \\ 1 & 2 \end{vmatrix} = A' \tag{16}$$

and in the second case we have:

$$X^U = W^{-1}B^{-1}ABW = \begin{vmatrix} 2 & 5 \\ -1 & -2 \end{vmatrix} = A'^3, \tag{17}$$

which are both in $\Omega$. Collecting the information above we state:

PROPOSITION 3. *A maximal finite subgroup* $\Gamma$ *of* $\Omega$ *is conjugate to one of the following subgroups:* $D_4^* = \langle A, B\rangle$, $D_4' = \langle A', Y_2\rangle$.

**4. The Normalized Automorphisms.** Let $\psi: \mathbb{Z}D_4 \longrightarrow \mathbb{Z}D_4$ be the function defined on the generators of $D_4$ by:

$$\begin{aligned} \psi(a) &= 2a - a^3 - b + ab + a^2b - a^3b, \\ \psi(b) &= a - a^3 + ab + a^2b - a^3b. \end{aligned} \tag{18}$$

since $\psi(a)^4 = \psi(b)^2 = \psi(b)\psi(a)\psi(b)\psi(a) = 1$, $\psi$ can be extended in an obvious way to $D_4$ and linearly to a morphism of $\mathbb{Z}D_4$.

Computing the matrix associated to $\psi$ in the basis of $\mathbb{Z}D_4$ given by the elements in $D_4$ it is easy to prove that $\psi$ is actually an automorphism.

Suppose that $\psi$ is the product of an automorphism of $D_4$ by an inner automorphism $\gamma_u$ defined by $\gamma_u = uxu^{-1}$, $\forall x \in \mathbb{Z}D_4$, with $u \in V(\mathbb{Z}D_4)$. Let $f: V(\mathbb{Z}D_4) \longrightarrow \Omega$ be the isomorphism in (8), and $\gamma_U : \Omega \longrightarrow \Omega$ the inner automorphism defined by $U = f(u)$. Then we have a commutative diagram:

$$\begin{array}{ccc} V(\mathbb{Z}D_4) & \xrightarrow{\gamma_u} & V(\mathbb{Z}D_4) \\ \Big\downarrow f & & \Big\downarrow f \\ \Omega & \xrightarrow{\gamma_U} & \Omega \end{array}$$

Therefore:

(19) $$\gamma_U(D_4^*) = f \circ \psi(D_4).$$

Finally: $f \circ \psi(a) = A'$ and $f \circ \psi(b) = Y_2$.

So in (19) we would have $\gamma_U(D_4^*) = D_4'$ contradicting proposition 3.

The example above shows that the answer to question $c$ is negative.

**References**


[1] S. D. BERMAN, *On the equation $x^m = 1$ in an integral group ring*, Ukran, Mat. Z., (1955) 253-261.

[2] J. A. COHN and D. LIVINGSTONE, *On the structure of group algebras* 1, Can. J. of Math., 17, 4, (1965), 583-593.

[3] G. HIGMAN, *The units of group rings*, Proc. London Math. Soc., 2, 4, (1940), 231-248.

[4] I. HUGHES and K. R. PEARSON, *The group of units of the integral group ring $\mathbb{Z}S_3$*, Can. Math. Bull., 15, 4, (1972), 529-534.

[5] M. NEWMAN, Integral Matrices, Academic Press, New York, 1972.

[6] C. POLCINO, *On the nilpotency of the group of units of group rings*, Anais. Acad. Brasileira de Ciências, to appear.



Instituto de Matemática e Estatística
Universidade de São Paulo
São Paulo - BRASIL